

BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-333110

(43)Date of publication of application : 30.11.2001

(51)Int.Cl.

H04L 12/66

H04L 9/36

H04L 12/46

H04L 12/28

H04L 12/56

H04Q 7/38

(21)Application number : 2000-151434

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 23.05.2000

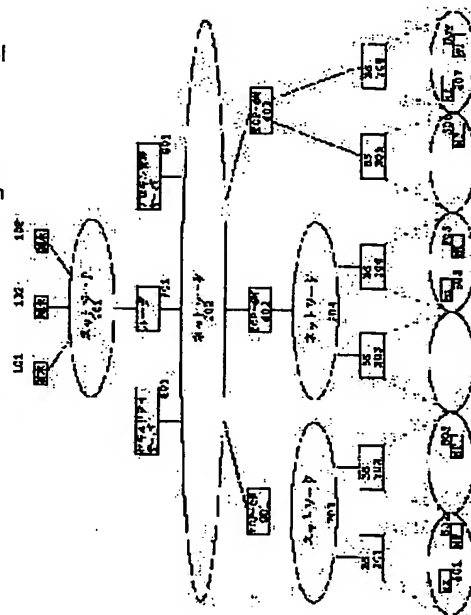
(72)Inventor : TAKAGI MASAHIRO
ISHIYAMA MASAHIRO

(54) GATEWAY DEVICE, COMMUNICATION EQUIPMENT, CONTROLLER, AND COMMUNICATION CONTROL METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a repeater, a communication equipment, a controller and a communication control method by which a wireless terminal and a wired terminal can make communication while keeping the security.

SOLUTION: A network 201 accommodates TCP/IP terminals 101-103, and interconnects a network 202 by a router 701 for switching IP packets. The network 202 accommodates networks 203, 204 with TCP-GW 401, 402 and base stations 305, 306 by a TCP-GW 403. The network 202 has a security server 601. The networks 203, 204 respectively contain base stations 301, 302 and base stations 303, 304. Mobile terminals 501, 502 exist in the base station 301, a mobile terminal 503 exists in the base station 302, mobile terminals 504, 505 exist in the base station 304, a mobile terminal 506 exists in the base station 305, and mobile terminals 507, 508 exist in the base station 306. The mobile terminals 501-508 are TCP/IP terminals.



LEGAL STATUS

[Date of request for examination]

07.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3730480

[Date of registration]

14.10.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-333110
(P2001-333110A)

(43) 公開日 平成13年11月30日 (2001. 11. 30)

(51) Int.Cl. ⁷	識別記号	F I	テレポート ⁸ (参考)
H 0 4 L	12/66	H 0 4 L	11/20 B 5 J 1 0 4
	9/36		9/00 6 8 5 5 K 0 3 0
	12/46		11/00 3 1 0 C 5 K 0 3 3
	12/28		11/20 1 0 2 A 5 K 0 6 7
	12/56	H 0 4 Q	7/04 D

審査請求 未請求 請求項の数12 O L (全 16 頁) 最終頁に続く

(21) 出願番号 特願2000-151434(P2000-151434)

(22) 出願日 平成12年5月23日 (2000. 5. 23)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 高木 雅裕

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(72) 発明者 石山 政浩

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(74) 代理人 100081732

弁理士 大胡 典夫 (外2名)

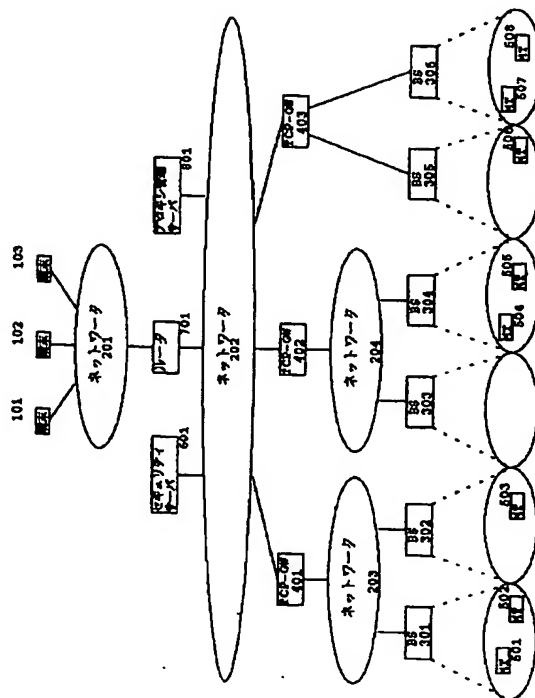
最終頁に続く

(54) 【発明の名称】 ゲートウェイ装置、通信装置、制御装置、および通信制御方法

(57) 【要約】

【課題】 セキュリティを維持しつつ、無線端末装置と有線端末装置間で通信を行う中継装置、通信装置、制御装置および通信制御方法の提供。

【解決手段】 ネットワーク201はTCP/IP端末101～103を収容し、IPパケットを交換するルータ701によってネットワーク202と相互接続される。ネットワーク202はTCP-GW401と402とによってネットワーク203、204を、TCP-GW403によって基地局305と306を収容する。ネットワーク202はセキュリティサーバ601を持つ。ネットワーク203と204は、それぞれ基地局301と302、基地局303と304を収容する。基地局301には移動端末501と502、基地局302には移動端末503、基地局304には移動端末504と505、基地局305には移動端末506、そして基地局306には移動端末507と508が存在する。移動端末501～508はTCP/IP端末である。



【特許請求の範囲】

【請求項 1】無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために、前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関する情報を保持する第 1 のセキュリティ情報保持手段と、

前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信を中継する際に前記第 1 セキュリティアソシエーションに関する情報を利用して前記無線端末装置もしくは前記有線端末装置に受信される暗号化された情報を復号化する情報復号化手段と、
前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、
前記中継手段が送信する情報を前記第 1 のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段とを具備したことを特徴とするゲートウェイ装置。

【請求項 2】無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、前記無線端末装置と前記有線端末装置との間で情報の認証を保証した通信を行うために、前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関する情報を保持する第 1 のセキュリティ情報保持手段と、

前記無線端末装置と前記有線端末装置との間で前記認証を保証された情報を前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、

前記中継手段が中継する前記認証が保証された情報および前記中継手段が必要に応じて新たに生成した情報に対して前記第 1 のセキュリティアソシエーションに関する情報を利用して、前記認証が保証された情報を保証する認証情報を付加する認証情報手段とを具備したことを特徴とするゲートウェイ装置。

【請求項 3】無線網に収容された無線端末装置もしくは有線網に収容された有線端末装置のいずれかに設けられ、

前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第 2 のセキュリティアソシエーションに関する情報を、前記無線端末装置と前記有線端末装置との間でトランスポート層以上の情報を用いた中継を行うゲートウェイ装置に提供するセキュリティ情報提供手段を具

備したことを特徴とする通信装置。

【請求項 4】前記第 1 乃至前記第 2 のセキュリティアソシエーションに関する情報は、前記無線端末装置と前記有線端末装置との間でトランスポート層以上の情報の通信を行う際に前記情報のセキュリティを管理するセキュリティサーバから前記ゲートウェイ装置に提供されることを特徴とする請求項 3 に記載の通信装置。

【請求項 5】無線網に収容された無線端末装置と有線網に収容された有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第 2 のセキュリティアソシエーションに関する情報を生成するセキュリティ情報生成手段と、
前記生成された第 1 乃至第 2 のセキュリティアソシエーションを前記無線端末装置乃至前記有線端末装置に配布するセキュリティ情報配布手段とを具備したことを特徴とする制御装置。

【請求項 6】無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継の制御を行う制御装置において、前記無線端末装置と前記有線端末装置に設けられた検索鍵に対する、前記無線端末装置乃至前記有線端末装置に設けられた検索鍵に対して、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第 2 のセキュリティアソシエーションに関する情報を検索し抽出するセキュリティ情報検索手段を具備したことを特徴とする制御装置。

【請求項 7】無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行う通信装置において、前記情報の内容に基づいて前記無線端末装置と前記有線端末装置との間で中継処理を行う中継手段を動作させるか否かを選択し、

前記中継手段を動作させる場合には前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第 2 のセキュリティアソシエーションに関する情報を用いて通信を行い、

前記中継手段を動作させない場合には前記無線端末装置と前記有線端末装置との間で通信を行うための第3のセキュリティアソシエーションに関する情報を設定し通信を行わせる選択手段を具備したことを特徴とする通信装置。

【請求項8】無線網に收容された無線端末装置と有線網に收容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、

第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を、第2のゲートウェイ装置に引き渡す工程と、

前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第1のゲートウェイ装置から前記第2のゲートウェイ装置に変化して経由された場合に、前記第1のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第1及び第2のセキュリティアソシエーションに関する情報を利用して前記第2のゲートウェイ装置において動作される工程とを有することを特徴とする通信制御方法。

【請求項9】無線網に收容された無線端末装置と有線網に收容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、

第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を、第2のゲートウェイ装置に引き渡す工程と、

前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第1のゲートウェイ装置から前記第2のゲートウェイ装置に変化して経由された場合に、前記第1のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第1及び第2のセキュリティアソシエーションに関する情報及び前記トランスポート層以上の状態を利用して前記第2のゲートウェイ装置におい

て動作される工程とを有することを特徴とする通信制御方法。

【請求項10】無線網に收容された無線端末装置と有線網に收容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、第1のゲートウェイ装置を通過した前記情報をカプセル化する第2のゲートウェイ装置と、

前記カプセル化された情報からカプセルを取り除き、前記カプセルが取り除かれた情報を前記トランスポート層以上の情報を利用して中継を行う必要があるか否かを判断し、必要な場合には中継を行う第3のゲートウェイ装置と、前記第3のゲートウェイ装置から送られた情報をカプセル化するカプセル化手段とを具備したことを特徴とするゲートウェイ装置。

【請求項11】ネットワークによって相互に通信可能な第1の通信装置と第2の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、

前記第1の通信装置と第2の通信装置との間で秘匿性を保証する通信のために、前記第1の通信装置と第2の通信装置との間に設定される第1のセキュリティアソシエーションに関する情報を保持する第1のセキュリティ情報保持手段と、

前記第1の通信装置と第2の通信装置との間で秘匿性を保証する通信を中継する際に前記第1のセキュリティアソシエーションに関する情報を利用して、前記第2の通信装置もしくは第2の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、

前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第1のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段とを具備したことを特徴とするゲートウェイ装置。

【請求項12】ネットワークによって相互に通信可能な第1の通信装置と第2の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、

前記第1の通信装置と第2の通信装置との間で秘匿性を保証する通信のために、前記第1の通信装置と第2の通信装置との間に設定される第1のセキュリティアソシエーションに関する情報を保持する第1のセキュリティ情報保持手段と、

前記第1の通信装置と第2の通信装置との間で秘匿性を保証する通信を中継する際に前記第1のセキュリティアソシエーションに関する情報を利用して、前記第2の通信装置もしくは第2の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、

前記復号化された情報に基づいて前記トランスポート層

以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第1のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段とを具備したことを特徴とするゲートウェイ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、トランスポート層を利用する通信に介在する中継装置、通信装置、制御装置および通信制御方法に関する。

【0002】

【従来の技術】近年無線によって音声信号のみならず、データ通信も行う要求が高まっている。TCP (Transmission Control Protocol) は、有線データ通信において信頼性のあるトランスポート層プロトコルとして広く使われているが、このプロトコルをそのまま無線に適用すると以下のような問題が発生する。

【0003】有線通信におけるTCPパケット損失はネットワークの輻輳を意味するため、TCPはパケット損失を検出するとデータの送出レートを下げて輻輳を回避するように設計されている。パケット損失は、同一シーケンス番号を持つACKが指定された数（通常はオリジナルに加えて3個）以上受信された場合、およびRTTとその偏差から定められるタイムアウトした場合に検出される。

【0004】このため無線区間のエラーおよびハンドオフによるTCPパケット損失、乃至はリンク層でのエラー回復に時間がかかった場合も輻輳と解釈されるので、必要以上に輻輳回避を行う結果、スループットが利用できる無線帯域以下に低下するケースが多くなる。また、無線区間のエラーをエンド・エンドでTCPによって再送すると、有線部分の帯域が無駄であるし時間もかかる。また、リンク層がエラー回復をしている場合は同じデータを重複して送ることになる。

【0005】このような問題を解決するために、有線側端末と無線側端末の間に（多くの場合は無線と有線の境界部分に）、TCPの性能を向上させるためのプロキシ（PEP: Performance Enhancement Proxy）を挿入する方法が提案されている。

【0006】Split Connectionによる方法は、TCPコネクションをProxy（以下ではTCP-GWと呼ぶ）に於いて、有線側TCPコネクションと無線側TCPコネクションとに分割する方法である。有線側から無線側端末にデータを送信する場合を想定する。

【0007】TCP-GWは無線側端末の代わりに有線側端末にACKを返すので、無線のエラーの影響（パケット損失乃至大きな遅延変動）は、有線側端末から隠蔽される。TCPデータパケットが失われた場合には、TCP-GWが有線側端末の代わりにデータの再送を行う。無線側のTCPは無線用にチューニングしたものであっても良い。例えば、無線側

TCPはselective ACKオプション（IETF RFC2018）を使って、高いパケット損失率でも性能が大きく劣化しないようにしたものであっても良い。また、輻輳制御のアルゴリズムを変更して、TCPパケット損失があっても、帯域を絞り過ぎない用にしたものであってもよい。

【0008】Snoop proxyによる方法は、TCP-GWがTCPコネクションを終端とみなしてしまうので、TCPのエンド・エンドセマンティクス（TCPのACKが送信端末に戻って来た場合には、そのACKのシーケンス番号までは受信端末に到達している）を破るという問題に対応するものである。Snoop proxyは、TCPデータパケットをバッファするが、その時点では送信端末にACKは返さない。本来の受信端末からのACKが帰って来た時点でACKを送信端末に中継し、バッファしていたTCPデータパケットを廃棄する。但し、ACKが重複ACKであり、本来の送信端末からの再送をトリガするものである場合、重複ACKは廃棄して、Snoop proxyがTCPデータパケットの再送を行う。また、Snoop proxyはタイムアウト再送も行う。このようにして、無線エラーの影響の大部分を、送信端末から隠蔽する。

【0009】一方で、このような無線データ通信は、近隣の誰かが無線信号を傍受可能であり、かつ移動環境で使用するケースが多いため、セキュリティに対する要求も高くなる。

【0010】インターネットにおけるセキュリティ確保の一方法として、IPSecによるものがある（IETF RFC2401, 2402, および2408など）。セキュリティは様々なレイヤで提供されるが、IPSecはIP層でセキュリティを確保するための方式である。IPSecでは、（1）IPヘッダの経路上で変更されない部分と、（2）IPペイロードに対してデータが経路上で改竄されていないことと、

（3）そのデータが本来の送信者によって生成されたこと、を保証する機能がある。このためには、AH（Authentication Header）を、IPヘッダとIPペイロードとの間に挿入しなければならない。また、IPペイロードに対して、秘匿性、改竄のないこと、および送信者による生成を保証する機能もある。このためには、ESP（Encapsulating Security Payload）を用いる。なお、AHとESPを組み合わせて使うこともできる。

【0011】また、IPSecやMobile IPでは、IPSecやMobile IPの機能を持つゲートウェイ装置やエージェント装置で、本来のパケットを別のパケットに包んで（カプセル化）して、ゲートウェイ装置やエージェント装置、乃至は本来のパケットの目的地である端末まで送信する技術が利用される。本来のパケットがカプセル化された状態で送る経路をトンネルと表現する。

【0012】

【発明が解決しようとする課題】以上説明したように、無線網に収容された無線側端末装置と有線網に収容された有線側端末装置との間で通信を行う際に、TCP-GW乃至Snoo

p proxyのようなTCPの性能を向上させるための装置とIP Secのようなセキュリティを提供する方法とは、共に無線データ通信環境での要求が高いが、このような装置と方法とを組み合わせる使用する場合には以下に説明するような問題があった。

【0013】つまり、TCPヘッダはIPSecによって保護されているIPペイロードに含まれるが、TCPの性能を向上させるProxyは、TCPヘッダに含まれる情報を知り、かつ場合によって変更しなければならないことが問題である。また、送信されるデータに改竄のないことを保証すると、TCP-GWが本来の受信端末に代わってACKを送信することはできなくなる。これはTCP-GW自身がACK情報を生成する必要が生じてくるためである。更に送信されるデータに秘匿性を要求すると、TCP-GW乃至SnoopProxyはTCPヘッダの情報が読み取れないので、有効な動作が不可能になる。

【0014】また、IPSecやMobileIPなどで利用される「トンネル」の途中にProxy装置がある場合、このproxy装置は有効に機能しない。なぜなら、例えばTCP-GWがカプセル化されたパケットを処理するべきか否かのフィルタにかけるために、カプセル化しているパケットのヘッダを調べても、そのヘッダはペイロードがTCPパケットであることを表示していないからである。

【0015】そこで、本発明は上記従来の問題点に鑑みてなされたもので、TCP-GWやSnoopに代表されるProxy装置と、IPSecに代表されるセキュリティプロトコルとを組み合わせることによって、セキュリティを維持しつつ無線端末装置と有線端末装置とのデータ通信を効率よく行い、またIPSecやMobileIPなどで利用される「トンネル」を通るカプセル化されたパケットに対しても有効に機能するゲートウェイ装置、通信装置、制御装置、および通信制御方法の提供を目的とする。

【0016】

【課題を解決するための手段】以上に述べた課題を解決するため、本発明におけるゲートウェイ装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために、前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報を保持する第1のセキュリティ情報保持手段と、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信を中継する際に前記第1セキュリティアソシエーションに関する情報を利用して前記無線端末装置もしくは前記有線端末装置に受信される暗号化された情報を復号化する情報復号化手段と、前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第1のセキュリティアソシエーションに関する情報を

利用して秘匿化する情報暗号化手段とから構成される。

【0017】また、本発明におけるゲートウェイ装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、前記無線端末装置と前記有線端末装置との間で情報の認証を保証した通信を行うために、前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報を保持する第1のセキュリティ情報保持手段と、前記無線端末装置と前記有線端末装置との間で前記認証を保証された情報を前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が中継する前記認証が保証された情報および前記中継手段が必要に応じて新たに生成した情報に対して前記第1のセキュリティアソシエーションに関する情報を利用して、前記認証が保証された情報を保証する認証情報を付加する認証情報手段とから構成される。

【0018】また、本発明の通信装置は、無線網に収容された無線端末装置もしくは有線網に収容された有線端末装置のいずれかに設けられ、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を、前記無線端末装置と前記有線端末装置との間でトランスポート層以上の情報を用いた中継を行うゲートウェイ装置に提供するセキュリティ情報提供手段とから構成される。

【0019】また、本発明における制御装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を生成するセキュリティ情報生成手段と、前記生成された第1乃至第2のセキュリティアソシエーションを前記無線端末装置乃至前記有線端末装置に配布するセキュリティ情報配布手段とから構成される。

【0020】また、本発明の制御装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継の制御を行う制御装置において、前記無線端末装置と前記有線端末装置に設けられた検索鍵に対する、前記無線端末装置乃至前記有線端末装置に設けられた検索鍵に対して、前記無線端末装置と前記有線端末装置との間で秘匿性を保証

する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を検索し抽出するセキュリティ情報検索手段とから構成される。

【0021】また、本発明における通信装置は、無線網に收容された無線端末装置と有線網に收容された有線端末装置との間でトランスポート層以上の情報の中継を行う通信装置において、前記情報の内容に基づいて前記無線端末装置と前記有線端末装置との間で中継処理を行う中継手段を動作させるか否かを選択し、前記中継手段を動作させる場合には前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を用いて通信を行い、前記中継手段を動作させない場合には前記無線端末装置と前記有線端末装置との間で通信を行うための第3のセキュリティアソシエーションに関する情報を設定し通信を行わせる選択手段とから構成される。

【0022】また、本発明の通信制御方法は、無線網に收容された無線端末装置と有線網に收容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を、第2のゲートウェイ装置に引き渡す工程と、前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第1のゲートウェイ装置から前記第2のゲートウェイ装置に変化して経由された場合に、前記第1のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第1及び第2のセキュリティアソシエーションに関する情報を利用して前記第2のゲートウェイ装置において動作される工程とを有する。

【0023】また、本発明における通信制御方法は、無線網に收容された無線端末装置と有線網に收容された有

線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を、第2のゲートウェイ装置に引き渡す工程と、前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第1のゲートウェイ装置から前記第2のゲートウェイ装置に変化して経由された場合に、前記第1のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第1及び第2のセキュリティアソシエーションに関する情報及び前記トランスポート層以上の状態を利用して前記第2のゲートウェイ装置において動作される工程とを有する。

【0024】また、本発明におけるゲートウェイ装置は、無線網に收容された無線端末装置と有線網に收容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、第1のゲートウェイ装置を通過した前記情報をカプセル化する第2のゲートウェイ装置と、前記カプセル化された情報からカプセルを取り除き、前記カプセルが取り除かれた情報を前記トランスポート層以上の情報を利用して中継を行う必要があるか否かを判断し、必要な場合には中継を行う第3のゲートウェイ装置と、前記第3のゲートウェイ装置から送られた情報をカプセル化するカプセル化手段とから構成される。

【0025】また、本発明におけるゲートウェイ装置は、ネットワークによって相互に通信可能な第1の通信装置と第2の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、前記第1の通信装置と第2の通信装置との間で秘匿性を保証する通信のために、前記第1の通信装置と第2の通信装置との間に設定される第1のセキュリティアソシエーションに関する情報を保持する第1のセキュリティ情報保持手段と、前記第1の通信装置と第2の通信装置との間で秘匿性を保証する通信を中継する際に前記第1のセキュリティアソシエーションに関する情報を利用して、前記第2の通信装置もしくは第2の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第1のセキュリティアソシエーションに関する情報を利用して秘匿化(暗号化)する情報暗号化手段とから構成される。

【0026】また、本発明におけるゲートウェイ装置は、ネットワークによって相互に通信可能な第1の通信装置と第2の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、前記第1の通信装置と第2の通信装置との間で秘匿性を保証する通信のために、前記第1の通信装置と第2の通信装置との間に設定される第1のセキュリティアソシエーションに関する情報を保持する第1のセキュリティ情報保持手段と、前記第1の通信装置と第2の通信装置との間で秘匿性を保証する通信を中継する際に前記第1のセキュリティアソシエーションに関する情報を利用して、前記第2の通信装置もしくは第2の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第1のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段とから構成される。

【0027】なお、無線通信端末および有線通信端末は、それら装置と情報の送受信もしくは中継がなされるサーバを含んだものであっても良い。また、通信装置は無線通信端末、有線通信端末乃至ルータであっても良い。

【0028】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【0029】図1は本発明のネットワーク構成図であり、ルータ701を挟んで、ネットワーク201側とネットワーク202側とに分けられる。これらの間でネットワーク運営の主体が異なっても構わない。ネットワーク201は有線網に有用されたTCP/IP端末101～103（有線端末装置）を収容し、IPパケットを交換するルータ701によってネットワーク202と相互接続されている。ここで、ネットワーク201と類似のネットワークが複数ネットワーク202に接続されていても良い。また、ネットワーク201がネットワーク202以外のネットワークと相互接続されていても良い。ネットワーク202側は移動をサポートしているものとする。但し、移動の有無は特許の本質とは無関係である。移動はMobileIPのようなIP層による実現、セルラー網のようなリンク層による実現などがあるが、その方法も問わない。移動を実現するために必要な要素は図示していない。ネットワーク202はTCP-GW401と402とによってネットワーク203と204とを、TCP-GW403によって基地局305と306とを、それぞれ収容する。

【0030】TCP-GWはSnoop ProxyのようなTCPを意識したリンク層再送機能を持つノードであっても良いし、更に一般的なプロキシ装置であっても構わないが、以下ではTCP-GWで代表する。更にネットワーク202はセキ

ュリティサーバ601を持つ。ネットワーク203と204は、それぞれ基地局301と302、基地局303と304を収容する。基地局301のエリアには無線網に収容された移動端末501と502、基地局302のエリアには無線網に収容された移動端末503、基地局304のエリアには無線網に収容された移動端末504と505、基地局305のエリアには無線網に収容された移動端末506、そして基地局306のエリアには無線網に収容された移動端末507と508が存在する状態を示している。移動端末501～508（無線端末装置）はTCP/IP端末である。

【0031】このような状況下で、例えば端末101と移動端末501の間でIPSecを利用してセキュリティを保証したTCP/IP通信を行う場合を想定する。IPSecによる通信を行うためには、端末101と移動端末501との間にIPSec SA（Security Association、以下SAと記す）が確立されている必要がある。

【0032】SAは一方方向の関係を示すので、双方方向の関係には2つのSAが必要となる。1つのSAに適用されるセキュリティプロトコルは1つに制限される。但し、必要なら2点の間で複数のSAを設定しても良い。SAを識別する情報は、（1）SPI（Security Parameter Index）、（2）IP destination address、（3）Security protocol identifierの3つである。SPIはローカルで一意的なビット列である。SPIは、AHおよびESPヘッダに含まれ、受信側が受信パケットを処理するために必要なSAを決定するために使われる。IP destination addressはSAの終点を示す。SAの終点はエンドユーザシステムであっても、ファイアウォールのようなものであっても良い。Security protocol identifierは、SAがAH乃至ESPを使うか否かを示す。

【0033】セキュリティアソシエーションデータベース（SAD）には、以下のような情報が含まれる。

【0034】・シーケンス番号カウンタ：AH乃至ESPヘッダのシーケンス番号フィールドを生成するために使用される。

【0035】・シーケンス番号カウンタオーバフロー：オーバフローした場合は、それ以上のパケット送信は禁止される。

【0036】・Anti-reply ウィンドウ：AHまたはESPパケットが第3者による再送でないことを保証するために、そのシーケンス番号は、ここで指定されるスライディングウィンドウの範囲になければならない。

【0037】・AH情報：認証アルゴリズム、鍵、鍵の生存時間、およびAHに関連するパラメータ。

【0038】・ESP情報：暗号化と認証アルゴリズム、鍵、初期化の値、鍵の生存時間、およびESPに関連するパラメータ。

【0039】・SAの生存時間：このSAが新たなSAで置き換えられなければならない、時間インターバル、乃至は

10

20

30

40

50

バイト数。およびこのような置き換えを行わなければならないか否かの指定。

【0040】・IPSecプロトコルモード:トンネル、トランスポート乃至ワイルドカードモード。

【0041】・Path MTU:観測されたパスの最大transmission unit (IPフラグメントなしでそのパス経由で伝送できる最大サイズ)。およびその情報の新しさ。

【0042】ユーザのポリシーによって、IPSecをいかにIPトラフィックに適用するかを決めることができる。つまりIPSecを適用するか否か、適用するとすればどのSAを利用するかを選択できる。このような情報はセキュリティポリシーデータベース (SPD) に含まれている。

【0043】SPDのエントリは、以下のselectorによって定められる。

【0044】・Destination IP address:範囲を示すものであっても良い。

【0045】・Source IP address:範囲を示すものであっても良い。

【0046】・User ID:システムのユーザ識別子。

【0047】・Data sensitivity level:秘密乃至そうでないかなど。

【0048】・トランスポート層プロトコル:UDP, TCPなどを指定するプロトコル番号。

【0049】・IPSec プロトコル:AH, ESP乃至AH/ESP。

【0050】・Source and destination ports:TCP乃至UDPのポート番号。

【0051】・IPv6 class, IPv6 flow label
・IPv4 Type of Service (TOS)

このように識別されるSPDの各エントリには、1つ以上のSAが対応している。

【0052】SAは手動で設定しても良いが、Internet Key Exchange (IKE) によって自動的に設定することも可能である。IKEは2つのフェーズに分けられる。フェーズ1では、IKE SAを確立しその後の通信の安全を図る。フェーズ2では、IKE SAの下で、AH乃至はESPのためのSAのパラメータを交換する。

【0053】さて、TCP-GWに代表されるプロキシ機能が機能するためには、TCP-GWがSAの少なくとも一部の情報を知っている必要がある。この情報とはより具体的には、暗号化を解いて必要な処理後に再び暗号を掛けるために必要な情報であり、また、プロキシがパケットを生成する場合にそのパケットを正しく認証された形式にするために必要な情報である。

【0054】このようなプロキシを機能させるための方法として、以下の方式が考えられる。

【0055】(方式1) 各種情報を手動で設定する。

【0056】(方式2) IKEのフェーズ2で交換されるSA情報から得る。つまり、IKE SAの情報を知っていてIPSec SA情報を傍受したエンティティがプロキシに情報を与える。

【0057】(方式3) SAのいずれかの端点から提供を受ける。

【0058】(方式4) プロキシ自ら、乃至セキュリティサーバがSA情報を生成し、各端点と必要ならプロキシに提供する。

【0059】以下では、方式3と方式4について詳しく述べる。

【0060】最初に(方式3)について述べる。端末101と移動端末501の間で、IKESAが確立されているとする。これから行おうとする通信に適用すべきIPSec SAは、確立されている場合と確立されていない場合がある。IPSec SA確立されていない場合は、端末101のセキュリティ情報管理1124 (図3参照、セキュリティ情報提供手段(請求項3))と移動端末501のセキュリティ情報管理1524 (図4参照、セキュリティ情報提供手段(請求項3))の間で、IKEのフェーズ2の手順でIPSec SAを確立すれば良い。セキュリティ情報管理1124 (選択手段(請求項7))、1524は、自らの持つSADとSPDに、このIPSec SA確立で発生した関連する情報を記憶する。なお、IPSec SAとして、プロキシの介在を許容するものと、許容しないものを設けても良い。更に、プロキシに暗号を解くことは許すが、新たなパケットの生成乃至パケット内容の変更は許容しないクラスがあっても良い。これはSPDのselectorのdata sensitivity levelに、その識別を行う分類を設けるのが自然であるが、例えばポート番号で識別しても良い。

【0061】以下では、プロキシの介在を許容するIPSec SAを主に扱う。プロキシの介在を許容しないIPSec SAについては、従来のIPSecと同様に動作する。

【0062】さて、端末101と移動端末501は、セキュリティサーバ601 (セキュリティ情報生成手段(請求項5)、セキュリティ情報配布手段(請求項5)、制御装置(請求項6))およびTCP-GW401~403を信頼できる装置として扱う。例えば、それらがある信頼できるネットワーク運営主体によって信頼できる装置として運用されている場合が想定できる。このネットワークのTCP-GWに代表されるプロキシ機能を利用するためには、セキュリティサーバ601にIPSec SA情報を提供する必要があることは、端末101乃至移動端末501の少なくともいずれか一方には認識されていることを仮定している。なお、セキュリティサーバ601でなく、TCP-GW401に直接IPSec SA情報を提供してもTCP-GWとして有効に動作できるが、利用する個別のプロキシを端末101乃至移動端末501が認識しなければならない。TCP-GWやSnoopなどは、本来その存在が端末から見えないので、これはあまり良い方法ではない。また、端末101、移動端末501のいずれが提供しても良いが、無線対応のプロキシを利用すべきであることをより容易に把握できる移動端末501が提供すると仮

定する。まず、これから送信するIPSec SA情報を保護するために、移動端末501とセキュリティサーバ601の間に何らかのセキュリティアソシエーションが必要である。セキュリティアソシエーションは、IPSecを使うと仮定する。移動端末501とセキュリティサーバ601の間で、最初にIKE SAを確立し、次にAHとESPの両方を用いるIPSec SAを確立する。このIPSec SAを用いて、移動端末501のセキュリティ情報管理1524から、セキュリティサーバ601のセキュリティ情報管理1624 (図5参照、セキュリティ情報生成手段(請求項5)、セキュリティ情報配布手段(請求項5)、セキュリティ情報検索手段(請求項6))に向けて、端末101と移動端末501の間のプロキシ介在を許容するIPSec SA情報を送信する。セキュリティ情報管理1624は、この情報をSPDとSADに記憶する。

【0063】図2はTCP-GWのブロック構成図であり、上述したSnoop Proxyのようなものであっても良くその場合の構成は異なる。また図3は端末101のブロック構成図であり、図4は移動端末501のブロック構成図であり、図5はセキュリティサーバ601のブロック構成図である。なお、図中の実線矢印はデータの流れ、破線矢印は制御の流れを示す。

【0064】以下で、TCP-GW401は、端末101と移動端末501の間のトラフィックを検出したことを契機に、IPSec SA情報をセキュリティサーバ601から取得する。ここでは、IKE SAによって、上記のプロキシ介在を許容するIPSec SAを確立するためのトラフィックを検出したとする。IKEはUDPのポート番号500を利用しているので、IP入力部1423でIPヘッダを見ていれば、この通信の存在がわかる。端末101と移動端末501の間の他の種類の通信であっても構わない。これらの存在は、端末101と移動端末501の間で、今後も何らかの通信が行われる可能性が高いことを示している。従って、TCP-GW401のセキュリティ情報管理1424

(第1のセキュリティ情報保持手段(請求項1, 2))が、セキュリティサーバ601のセキュリティ情報管理1624に対して、端末101と移動端末501の間のIPSec SAに関する情報を提供するように要求する。例えば端末101と移動端末501のIPアドレスの組を検索鍵として予めセキュリティサーバ601に記憶しておくことも一手法である。

【0065】セキュリティサーバ601のセキュリティ情報管理1624は、TCP-GW401のセキュリティ情報管理1424からの要求を受けた時点では、まだ端末101と移動端末501の間のIPSec SAを持っていないかも知れない。なぜなら、この要求はIPSec SAを設定するためのトラフィックを検出して行われたものだからである。セキュリティ情報管理1624は、そのような要求があったことをタイムアウトするまで記憶しておいて、要求にあうIPSec SA情報を得る度に、TCP-GW401のセ

キュリティ情報管理1424に、IPSec SA情報を提供する。

【0066】このようにして、TCP-GW401のセキュリティ情報管理1424が、セキュリティサーバ601のセキュリティ情報管理1624から、端末101と移動端末501の間のIPSec SAに関する情報を得ると、これをセキュリティ情報管理1424のSPDとSADに記憶する。更に、IP入力部1423でフィルタを設定して、端末101と移動端末501の間のプロキシ介在を許容するIPSec SAによるパケットでかつTCPの通信であるという条件にマッチする時には、TCP層まで上げるようにする。なお、IPSec SA情報要求がタイムアウトする時点で、更に端末101と移動端末501の間での通信がTCP-GW401を通過すると見込まれる場合には、要求を更新する。

【0067】次に、プロキシを許容するIPSec SAを利用して、端末101のPEP利用アプリケーション1162 (図3参照)と移動端末501のPEP利用アプリケーション1562 (図4参照)が通信を行う。なお、アプリケーションでプロキシを許容するか否かを分けているのは便宜的なもので、実際にはTCPのコネクション毎に使い分けが可能である。PEP利用アプリケーション1162がPEP利用アプリケーション1562に対して、TCPのコネクション設定を行うとする。PEP利用アプリケーション1162は、例えばUNIX (登録商標)のsocketインタフェースによって、OSに対してTCPコネクション設定を要求できる。この際、例えばsocketのオプションによって、このTCPコネクションをプロキシ介在を許容するか否かを指定できる。既に述べたように、ここではプロキシ介在を許容する。これは、例えばSPDエントリのData sensitivity level selectorの値として設定される。他のselectorの値は、destination IP addressとして移動端末501のIPアドレス、source IP addressとして端末101のIPアドレス、UserIDとしてPEP利用アプリケーション1162のユーザ識別子、Transport layer protocolとしてTCP、IPSec protocolとして例えばAH/ESP (他にAHあるいはESPが可能)、source/destination portとして適当なポート番号などとなる。IP出力部1122を監視しているセキュリティ情報管理1124は、出力IPパケット毎にSDPエントリを検索し、対応するIPSec SAを見付ける。Selectorが上記の値を持つパケットに対しては、既に述べたプロキシ介在を許容するIPSec SAが対応する。するとセキュリティ情報管理1124は、IPSec SAに指定されたアルゴリズムと鍵などによって、パケットを暗号化し認証のための情報を付加するように、暗号機能1126と認証機能1125を制御する。トランスポートモードとトンネルモードのうち、ここでは前者を利用するので、図6(a)のパケットを処理後のパケットは図6(b)に示すフォーマットになる。ここで、一般に暗号化後にはTCPヘッダ

とデータの境界は保存されない。また、AH認証対象は、IPヘッダの経路上での変化による結果を予測できない部分（例えばTTLなど）は含まない。

【0068】このように処理されたパケットは、有線IF出力部1142によってネットワーク201に送信され、更にルータ701、ネットワーク202を経由して、TCP-GW401に到着する。有線側IF入力部1446を経てIP入力部1423に到着したパケットは、SPI (Security Parameter Index)、IP destination address、Security protocol identifierの3つによって識別されるIPSec SAの指定に従って処理される。識別するパラメータの値は、セキュリティサーバ601から提供されたものであり、セキュリティ情報管理1424によってIP入力部に設定されている。セキュリティ情報管理1424が認証機能1425（認証情報手段（請求項2））と暗号機能1426（情報復号化手段（請求項1））、情報暗号化手段（請求項1））を制御して、図6（b）に示すIPSecパケットを、図6（a）に示す元のパケットの形に戻す。

【0069】元のパケットの情報からTCP中継処理を行うか否かをIP入力部1423が判断し、中継処理を行うものとしてTCP入力部1405に渡す。最も単純な判断基準はTCPなら全てTCP接続を利用して中継するというものであるが、他の属性も使用してTCPだがTCP情報を利用した中継をしないようにしても良い（IP中継となる）。このパケットは、その内容に応じて、TCP中継部1402（中継手段（請求項1、2））の有線→無線1407、TCP入力部1405および無線TCP出力部1408で処理される。例えば、SYNパケットなら、新たなTCPコネクションが設定されるものとして対応する状態を生成する。必要なら適当なオプションを追加するなどして、無線TCP出力部1408に中継する。更に、TCP出力部1404からSYN/ACKを返す（Snoopの場合は返さない）。別の例として、データパケットなら、後で再送する可能性があるため、バッファにコピーを蓄積してから、無線TCP出力部1408に渡す。更に、TCP出力部1404からそのデータパケットに対するACKを返す（Snoopの場合は返さない）。なお、ここで扱っているパケットは、TCP-GW401が生成したものを含め、全て端末101と移動端末501の間で送受信されているかのように、IPヘッダのアドレスフィールドが設定されている。つまり、TCPゲート401存在は隠されている。

【0070】無線TCP出力部1408およびTCP出力部1404は、パケットをIP出力部1422に渡す。セキュリティ情報管理1424は、パケットの情報からSPDのエントリを識別するselector情報を得て、SPDを検索して対応するIPSec SAを得る。このIPSec SAに関する情報をSADから取得して、それに応じて暗号機能1426と認証機能1425を制御して、再びパケットを図6

（b）に示すIPSecパケットの形にする。ここで同じパ

ケットであっても、TCP-GWに受信されたIPSecパケットと、TCP-GWから送信されるIPSecパケットの内容は一般に異なる。例えば、TCP-GW401は、ACKを中継するのではなく生成するので訂正のために付与されるIPSecのAHないしESPのシーケンス番号は一般に異なる。これらのパケットは、無線側IF出力部1443からネットワーク203へ、有線側IF出力部1445からネットワーク202へ、それぞれ送信される。

【0071】なお、Snoopの場合は、Snoop proxyに受信されたIPSecパケットと、Snoop proxyから送信されるIPSecパケットの内容は多くの場合同じにできる。

【0072】Snoopは重複ACKを中継せずに捨てることがあるが、これはIPネットワーク内で自然に失われるのと同じであり、IPSec的に特に問題無い。Snoopが本来のTCP送信ホストの代わりに再送を行うことがあるが、これはオリジナルのコピーを再送すれば良いが、IPSecのAnti-replyによって受信端末で捨てられる可能性がある。これを防ぐためには、認証のためのシーケンス番号が、Anti-replyウィンドウの範囲内に収まっている必要がある。これらの条件が満たされれば、Snoopの場合には、IPSecパケットから元のTCP/IPヘッダ情報を取り出せば良いのであって、一度オリジナルの形に戻したパケットを再びIPSecパケットに変更する必要は無い。従って、Snoop proxyに認証を掛けるために鍵情報を与えなければ、端末101と移動端末501の間で、情報の改竄がなかったことと、本来の送信者から送信されたパケットであることはIPSec的に保証できる。Snoop proxyに暗号を解くためのSA情報を持てば機能できる。

【0073】ネットワーク203へ送信されたパケットに注目すると、これは基地局301経由で移動端末501によって受信される。無線IF入力部1543を経てIP入力部1523に到着したパケットは、SPI (Security Parameter Index)、IP destination address、Security protocol identifierの3つによって識別されるIPSec SAの指定に従って処理される。セキュリティ情報管理1524が認証機能1525と暗号機能1526を制御して、図6（b）に示すIPSecパケットを、図6（a）に示す元のパケットの形に戻す。そして、パケットに載っていた情報は、PEP利用アプリケーション1562に渡される。

【0074】次に（方式4）、つまりセキュリティサーバ601がIPSec SA情報を生成し、端末101と移動端末501、およびTCP-GW401に生成したIPSec SA情報を渡す場合について述べる。

【0075】移動端末501のセキュリティ情報管理1124が、セキュリティサーバ601のセキュリティ情報管理1624に対し、端末101との間のプロキシの介在を許容するIPSec SA情報を生成するように依頼する。依頼にはIPSecなどでセキュリティの確保された通信路を用いる。セキュリティ情報管理1624は、依頼

に応じたIPSec SA情報を生成すると、これをセキュリティの確保された通信路で、移動端末501、端末101、およびTCP-GW401に提供する。移動端末501には、依頼の応答として提供すれば良い。端末101に対しては、セキュリティサーバ601から直接提供しても良いし、移動端末501から提供しても良い。TCP-GWに対しては、例えば移動端末501の位置情報から、TCP-GW401がIPSec SAを利用する可能性の高いと判断できれば、セキュリティサーバ601が自発的に送信すれば良い。さもなければTCP-GW401が、端末101と移動端末501の間の通信を検出してから、セキュリティサーバ601に要求することになる。全てのTCP-GW401~403に提供しても機能するが、効率は悪いし、セキュリティが破られる可能性も高くなる。これらの通信は、端末101、移動端末501、TCP-GW401、およびセキュリティサーバ601それぞれのセキュリティ情報管理1124、1524、1424、および1624の間で行われる。一旦、IPSec SAの情報がTCP-GW401に提供されれば、後の動作は（方式3）の場合と同様であるので省略する。

【0076】これから、移動端末（例えば移動端末501）の移動に伴いTCP-GWを変更するプロキシハンドオフ制御について述べる。このため、移動端末501で終端される中継対象のTCPコネクション状態の情報と、移動端末501に対応するIPSec SA情報を、前のTCP-GW（例えばTCP-GW401）から後のTCP-GW（例えばTCP-GW402）に引き継ぐ必要がある。TCP-GW402は、移動端末501を起点・終点とする通信を検出した際に、前のTCP-GWを何らかの方法で探して、ハンドオフ処理を行うために必要な情報を要求する。このために予め隣接するTCP-GWをお互いに認識しておくことが有効である。

【0077】例えば、（NR方式A）物理的な距離が近いTCP-GWを認識する、（NR方式B）ネットワーク的な距離（ホップ数、遅延など）が近いTCP-GWを認識する、といった方式が考えられる。

【0078】移動端末の物理的な移動によりハンドオフが必要になるとすると、（NR方式A）が望ましい。しかし、物理的な位置を知ることができない場合には、（NR方式B）を利用する場合もある。

【0079】（NR方式A）を実現するために、例えばプロキシ管理サーバ801を設ける。TCP-GW401は基地局301と302、TCP-GW402は基地局303と304、TCP-GW403は基地局305と306の物理的な位置を何らかの方法で知りえており、その情報をプロキシ管理サーバ801に通知する。プロキシ管理サーバ801は、TCP-GW401と402の間のハンドオフ、TCP-GW402と403の間のハンドオフが発生し得ると判断する。そして、TCP-GW401に対してはTCP-GW402がハンドオフ対象となること、TCP-GW402に対してはTCP-GW401と403がハンドオフ対象となること、TCP-GW

403に対してはTCP-GW402がハンドオフ対象となることを通知する。これらの処理は、TCP-GW401~403のTCPハンドオフ制御1410とプロキシ管理サーバ801によって行われる。もちろん、TCP-GW401~403に対して、これらの情報を手動で設定することも可能である。

【0080】また、（NR方式B）を実現するためには、例えば次のような手順が考えられる。

【0081】全てのTCP-GWが加入するマルチキャストグループを定義しておき、各TCP-GWのTCPハンドオフ制御1410がTTLを適当に制限したマルチキャストパケットを問い合わせるために送信する。これを受信した各TCPハンドオフ制御1410が送信元にユニキャストで応答することで、ホップ数の少ないTCP-GWを探すことができる。

【0082】さて、上述したように、端末101と移動端末501の間で、プロキシ介入を許容するIPSec SAの下で、TCP-GW401を介して、TCPによる通信を行っているとする。プロキシハンドオフに伴う情報の引渡しにはいくつかのバリエーションが考えられる。

・ハンドオフする可能性のあるTCP-GWに、予め渡せる情報は渡しておくか否か。予め渡すとすれば以下のような候補がある。

【0083】—中継対象端末：新しいTCP-GWがこの端末の通信を検出した時に、どのTCP-GWに問い合わせれば、必要な情報が得られるかがわかる。

【0084】—IPSec SA情報：ハンドオフ遅延の減少が見込める。

・ユニキャストで問い合わせるか、マルチキャストで問い合わせるか。

【0085】—ユニキャスト：前のTCP-GWである可能性のある全てのTCP-GWに個別に問い合わせる。上記中継対象端末情報またはIPSec SA情報を持っていれば、その情報を提供したTCP-GWに問い合わせる。

【0086】—マルチキャスト：前のTCP-GWである可能性のある全てのTCP-GWを含むマルチキャストグループを定義しておく。このマルチキャストグループ宛に問い合わせを送信する。

【0087】なお、ハンドオフに伴う通信は、原則としてセキュリティが確保された通信路によって行う。

【0088】ここで、TCP-GW401のセキュリティ情報管理1424から、TCP-GW402のセキュリティ情報管理1424に対して、予めIPSec SA情報が与えられているとする。TCP-GW401のセキュリティ情報管理1424は、セキュリティサーバ601から新たなIPSec SA情報を得ると、TCPハンドオフ制御1410に、そのIPSec SA情報を提供すべき先のTCP-GWを問い合わせる。この場合はTCP-GW402に提供すべきなので、TCP-GW401のセキュリティ情報管理1424は、TCP-GW402のセキュリティ情報管理1424に対して、そのIPSec SA

情報を提供する。TCP-GW 402のセキュリティ情報管理1424は、IPSec SA情報をSPDとSADに記憶すると共に、その提供元がTCP-GW 401であることと、その提供時間を記憶する。

【0089】移動端末501が基地局301のエリアから、基地局302のエリアを経て、更に基地局303のエリアへ移動したとする。するとTCP-GW 402が端末101と移動端末501の間の通信を検出する。TCP-GW 402のセキュリティ情報管理1424は、端末101と移動端末501の間のIPSec SA情報を、最近提供したものがTCP-GW 401であることを認識するので、TCPハンドオフ制御1410に対して、TCP中継のハンドオフに必要な情報は、TCP-GW 401から得られることを教える。また、TCP-GW 402のセキュリティ情報管理1424は、TCP-GW 403のセキュリティ情報管理1424に対して、対応するIPSec SA情報を通知する。以前から知っていたIPSec SA情報をこの時点で通知するのは、TCP-GW 403へのハンドオフの可能性が生じたからである。

【0090】TCP-GW 402のTCPハンドオフ制御1410は、TCP-GW 401のTCPハンドオフ制御1410から得た、端末101と移動端末501間のTCPコネクションの情報から、TCP 1401と無線TCP 1403に対してTCP中継に必要な情報を設定する。例えば、シーケンス番号やウィンドウ制御関連の情報、設定されているTCPオプション、バッファに一時記憶されているデータパケットなどである。TCP中継の再開にあたっては、TCPシーケンス番号がなるべく乱れ無いように行う。つまり、バッファに一時記憶されているデータパケットのTCPシーケンス番号が、端末101と移動端末501の間を流れているTCPデータパケットのシーケンス番号よりも小さければ、それらを先に中継する。その後のTCP中継処理、およびIPSec関連の処理は既に述べた手順に準ずる。

【0091】次に、端末102がIPSecの機能を持たないIP端末で、ルータ701がセキュリティサービスとして、ネットワーク102からネットワーク201へ出る、IPSecで保護されていないパケットを、IPSecのトンネルモードで保護する場合について述べる。特に、カプセル化されたパケットをプロキシで扱う方法について説明する。Mobile IPなど他のカプセル化の場合にも適用できる。

【0092】端末102と移動端末502の間の通信を想定する。移動端末502は、図4に構成を示すようなIPSec機能を持つ端末である。端末102は、図7に示すような構成でありIPSec機能を持たない端末である。この間で通信を行う際に、図8に構成を示すルータ701と移動端末502の間でIPSecを利用した通信を行う。このため、既に述べたものと同様な方式で、ルータ701と移動端末502の間のIPSec SAが確立され、更にセキュリティサーバ601を介して、プロキシ介在

を許容するIPSec SAの情報が必要なTCP-GW 401に提供される。この際には、IPSecのトンネルモードが用いられる。端末102と移動端末502の間のパケットに対応するIPSecパケットは、図9(a)に示す形になる。

【0093】TCP-GW 401での中継処理は既に述べた方式に準ずる。但し、セキュリティ情報管理1424の制御の下でIPSecを解いてカプセル化も外した後のパケットについては、IP入力部1423がTCP中継を行うか否かを判断し、必要な場合にTCP 1401にパケットを渡すことになる。また、パケットを送信する際はIPSecとカプセル化の処理を行う(図9(b)参照)。既に述べた方式との処理の切り替えは、SADから得たIPSec SA情報に含まれるIPSecプロトコルモードの値が、トランスポートモードであるか、トンネルモードであるかによって行うことができる。また、新しいIPヘッダが、カプセル化ヘッダであることを認識して行うこともできる。これは、例えばMobile IP (IETF RFC2002) によるHome AgentとForeignAgentの間のカプセル化されたTCP/IPパケットを扱うTCP-GWの場合など、一般にトンネルの中間にあるプロキシの場合にも適用できる。

【0094】なお、上記の実施の形態はその主旨を逸脱しない範囲で種々変形して実施できることは言うまでもない。例えば、IPv6に適用することも可能である。

【0095】また、有線端末と無線端末の間だけではなく、無線端末501と無線端末508の間の通信にも本発明が適用できることは明らかである。

【0096】

【発明の効果】以上述べたような本発明によれば、IPSecなどでセキュリティを保証した通信に対しても、TCP-GWやSnoopに代表されるプロキシを適用して無線環境下での性能の向上を図ることができる。

【図面の簡単な説明】

【図1】 本発明の中継装置、通信装置、制御装置を含んだネットワーク構成図。

【図2】 本発明のTCP-GWのブロック構成図。

【図3】 本発明の端末のブロック構成図。

【図4】 本発明の移動端末のブロック構成図。

【図5】 本発明のセキュリティサーバのブロック構成図。

【図6】 本発明のIPSec処理前後のパケットフォーマットの構成図。

【図7】 本発明の別の端末のブロック構成図。

【図8】 本発明のルータのブロック構成図。

【図9】 本発明のIPSec処理前後のパケットフォーマットの構成図。

【符号の説明】

101、102、103 端末

201、202、203、204 ネットワーク

301、302、303、304、305、306 基地局

401、402、403 TCP-GW

601 セキュリティサーバ

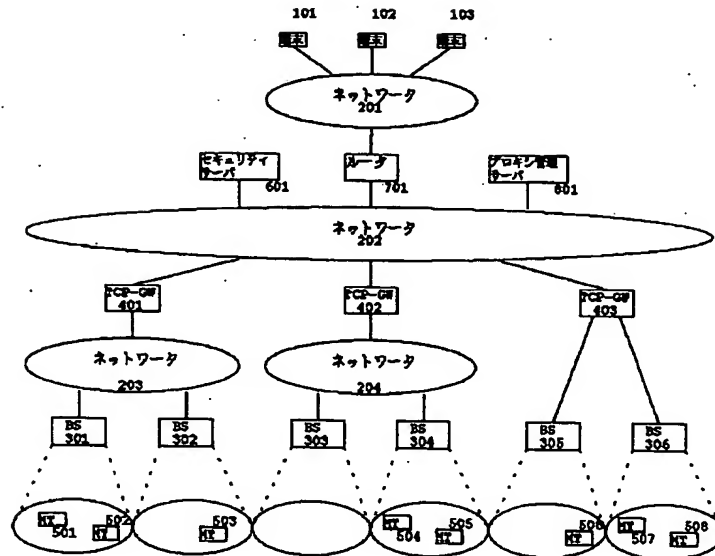
501、502、503、504、505、506、5

701 ルータ

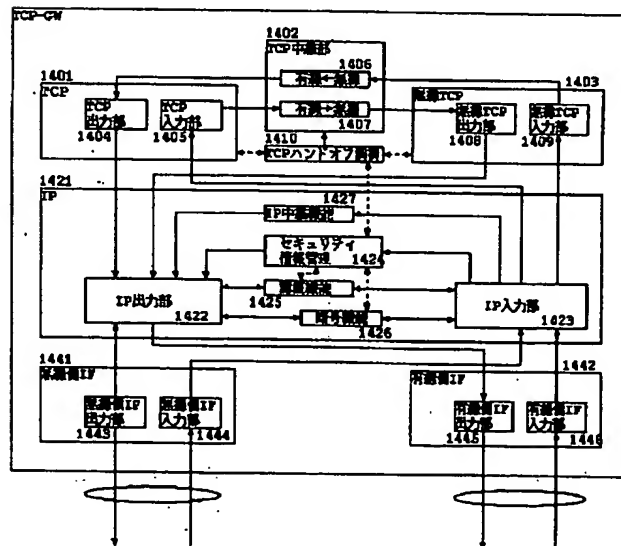
07、508 移動端末

801 プロキシ管理サーバ

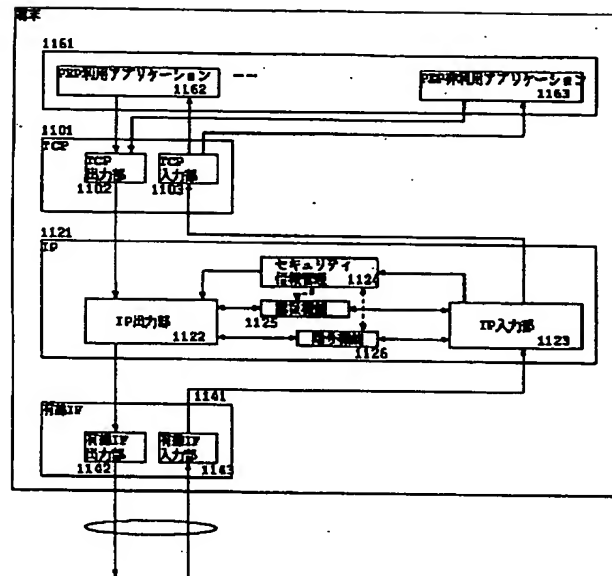
【図1】



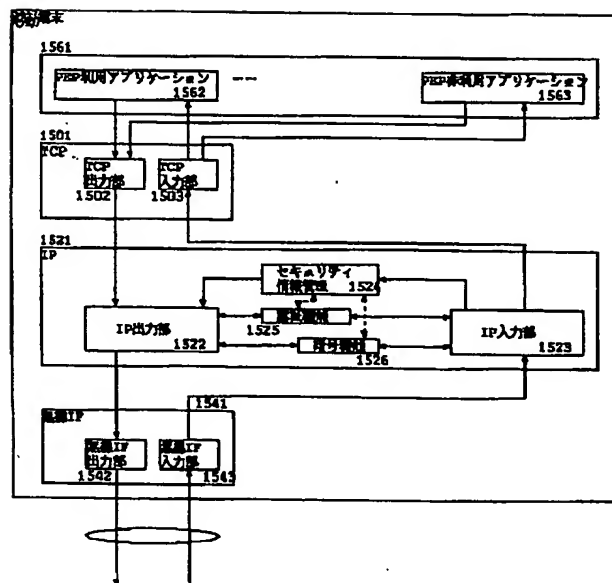
【図2】



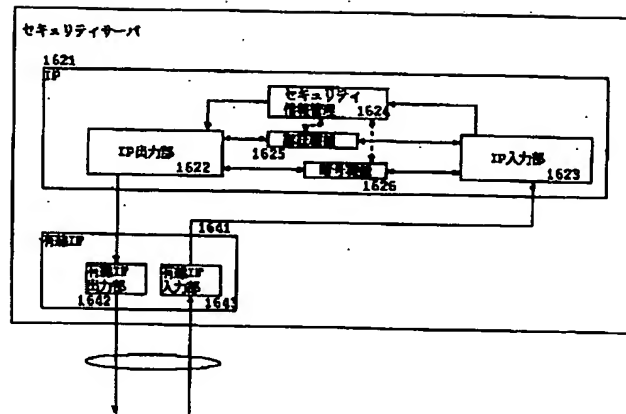
【図3】



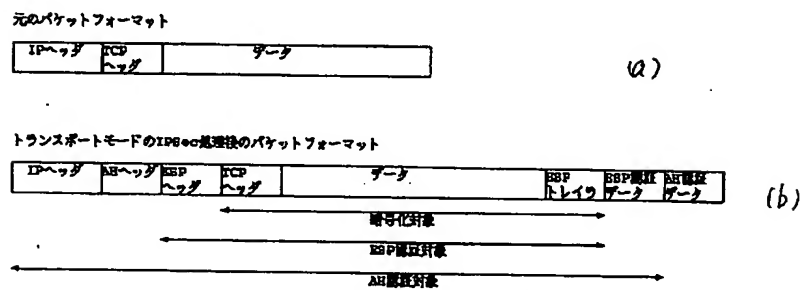
【図4】



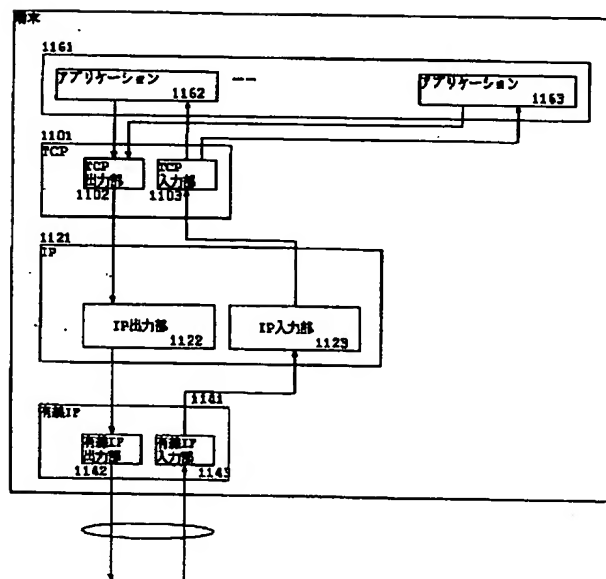
【図5】



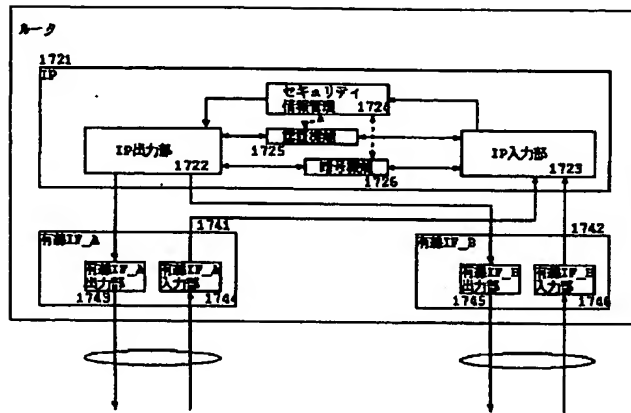
【图6】



【图7】

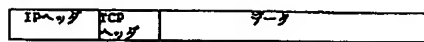


【図8】



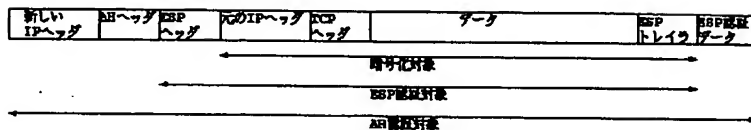
【図9】

元のパケットフォーマット



(a)

トンネルモードのIPSec処理後のパケットフォーマット



(b)

フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

テーマコード* (参考)

H 0 4 Q 7/38

Fターム(参考) 5J104 AA01 BA02 PA01 PA07
 5K030 GA15 HA08 HD03 JT02 JT09
 KA17 KA19
 5K033 AA08 CB08 DA05 DA19 DB10
 DB18
 5K067 AA35 BB21 DD57 EE02 EE10
 EE16 HH05 HH11 HH22 HH24
 HH36

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.